## REMARKS/ARGUMENTS

The Office Action mailed August 6, 2004 has been reviewed and carefully considered. Claims 1, 6, 10, 13, 22, 24, 25, 28, and 31 have been amended. Claims 1-34 are pending in this application, with claims 1, 13, 25, 28, and 31 being the only independent claims. Reconsideration of the above-identified application, as herein amended and in view of the following remarks, is respectfully requested.

Objections to the Specification and Claims:

In the Office Action mailed August 6, 2004, the specification is objected to because the sentence on page 14, lines 9-11, contains grammatical errors. The specification has been amended to correct the noted error. In view of the amendments, the objection to the specification should now be withdrawn.

Claim 24 is objected to as containing a minor informality. Claim 24 is amended so that it is drawn to an apparatus as is claim 23 from which it depends. In view of the amendments, the objection to claim 24 should now be withdrawn.

Rejections Under 35 U.S.C. §112:

Claim 6 stands rejected under 35 U.S.C. §112, second paragraph, because "the recorded data stream" has insufficient basis. Claim 6 is amended to recite -- stored encrypted packets of the data stream --, which has proper antecedent basis.

Claims 10-12 and 22-30 stand rejected under 35 U.S.C. §112, second paragraph, because the Examiner considers the IC tester, which is omitted from these claims, to be essential. It is respectfully submitted that the IC tester is part of preferred embodiment but is not essential (see page 12, lines 19-20). Nevertheless, claims 10, 20, 25 and 28 have each been amended to recite that the claimed readout path is connectable to an external IC tester.

Claims 10-12 and 22-30 stand rejected under 35 U.S.C. §112, second paragraph, because the Examiner states that the omitted step of disabling the path essential to functioning of the recording and playback device by the second irrevocable condition **when** the second irrevocable condition re-enables the readout path for at least a portion of the encryption key is essential. While this is desired, as indicated on page 3, lines 20-21 of the specification, there is no teaching or suggestion that this step is essential.

In view of the above amendments and remarks, it is respectfully requested that the rejection of claims 6, 10-12, and 22-30 under 35 U.S.C. §112, second paragraph, now be withdrawn.

Rejections over Prior Art

Claims 1, 2, 6, 7, 13, 14, 18, 19, 31, and 32 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,714,650 (Maillard).

Claims 3, 4, 5, 15, 16, 17, 33, and 34 stand rejected under 35 U.S.C. §103 as unpatentable over Maillard in view of U.S. Patent No. 5,963,646 (Fielder) and U.S. Patent No. 6,212,635 (Reardon).

Claims 8 and 20 stand rejected under 35 U.S.C. §103, as unpatentable over Maillard in view of U.S. Patent No. 5,852,290 (Chaney).

Claims 10-12 and 22-30 stand rejected under 35 U.S.C. §103 as unpatentable over Maillard in view of Fielder and Reardon and further in view of U.S. Patent No. 5,627,478 (Habersetzer) and U.S. Patent No. 6,105,136 (Cromer).

Claims 9 and 21 were found to contain allowable subject matter and would be allowable if rewritten in independent form. Although the finding of allowable subject matter is appreciated, the above rejections are traversed in view of the following remarks.

Before discussing the cited prior art and the Examiner's rejections of the claims in view of that art, a brief summary of the present invention is appropriate. The present invention relates to a method and device for recording digital data streams and restricting the distribution of copies recorded on such devices. More specifically, the present invention allows a user to record a digital broadcast for later viewing while simultaneously preventing illegal copying and distribution of the recorded digital broadcast (page 11, lines 3-6, of the present specification). According to the present invention, the digital broadcast is encrypted in the recording device with an encryption key unique to the recording device (page 3, lines 2-4; page 7, lines 5-8). The broadcast is stored in the encrypted state so that the copy would not play back intelligibly on other recorders (page 7, lines 9-10).

If a first recorder breaks down, the user requires the internal key of that first recorder to play back recorded copies on a new recorder. Accordingly, the present invention also provides a procedure for recovering the internal key 204 from the first recorder so that the internal key 204 can be programmed into another recorder (page 12, line 6 to page 14, line 14). To prevent abuse, the present invention provides a scheme for preventing operation of the first recorder once the internal key has been retrieved (page 14, lines 5-11).

Each of independent claims 1, 13, and 31, recites that a recording and playback device (1) receives packets of digital stream, (2) encrypts the received packets in the recording and playback device according to an encrypted key unique to the recording and playback device and (3) stores the encrypted packets.

It is respectfully submitted that Maillard fails to teach or suggest "encrypting the <u>received</u> packets in the recording and playback device according to an encryption key unique to the recording and playback device", as expressly recited in independent claims 1, 13, and 31.

Maillard discloses a device and method for recording scrambled digital data. According to Maillard, a decoder 13 is connected to a digital recording device 41 (col. 7, lines 30-31 of Maillard). A particular song (or other data stream such as a video) is scrambled prior to transmission by a control word (col. 7, lines 53-55). Each control word is encrypted using an encryption key $K_t$ associated with the song, the encrypted control word forming a characteristic ECM message (col. 7, lines 58-61; and col. 8, lines 6-9). Maillard further states that a ciphering unit 50 includes the encrypted key $K_t$ needed to decrypt the ECM message and a key $K_i$ associated with the identity of the disc reader 41 (col. 8, lines 9-13). The key $K_t$ is encrypted by the key $K_i$ forming an EMM message that is sent to the decoder 13 in Maillard (col. 8, lines 13-16).

Maillard scrambles the song at a central location using a control word. The control word is encrypted by a key $K_t$ and forms an ECM message. The key $K_t$ is encrypted by a key $K_i$ in a ciphering unit 50 to form an EMM message. The EMM message is sent to the decoder 13. Accordingly, the actual song is not encrypted, only the EMM. In addition, the encryption of the key $K_t$ is performed outside of the recording and playback device, in the ciphering unit 50. Therefore, Maillard fails to disclose, "encrypting the received packets in the recording and playback device according to an encryption key unique to the recording and playback device", as expressly recited in independent claims 1, 13, and 31. In view of the above remarks, independent claims 1, 13, and 31 are not anticipated by Maillard under 35 U.S.C. §102.

Furthermore, since Maillard teaches that the recorded data is scrambled by a key $K_t$, and that the key is encrypted outside the recording and playback unit, there is no teaching or suggestion for "encrypting the received packets in the recording and playback device according to an encryption key unique to the recording and playback device", as expressly recited in

independent claims 1, 13, and 31. Accordingly, claims 1, 13, and 31 are also allowable over Maillard under 35 U.S.C. §103.

In addition, independent claim 31 is directed to a set-top box. The encryption disclosed by Maillard does not occur in a set-top box. Rather, Maillard discloses that the encryption occurs in a broadcast center, as described above. According, claim 31 is allowable for these additional reasons.

Independent claims 25 and 28 are directed to a method and recorder which encrypts a digital data stream according to a unique key and stores the encrypted data stream. Independent claims 25 and 28 are amended to more definitely recite that the data stream is encrypted and stored in the recording and playback device. Accordingly, the readout path is disabled by a first irrevocable condition and the readout path is enabled by a second irrevocable condition which disables at least one feature essential for the recording and playback functions.

As described above with respect to independent claims 1, 13, and 31, Maillard fails to teach or suggest that the audio or video program itself is encrypted in the recorder before being recorded, as is now expressly recited in independent claims 25 and 28. It is respectfully submitted that Maillard also fails to teach or suggest a readout path for reading the internal key, wherein (1) the readout path is disable by a first irrevocable condition, and (2) the readout path is re-enabled by a second irrevocable condition, at least one feature essential for the recording and playback functioning of the recorder being arranged to be disabled by the second irrevocable condition.

The Examiner takes official notice that means for restricted reading of an encrypted key based on a set of conditions is a conventional feature because access privileges, request validity, memory integrity validation are known. However, these means are <u>not</u> the same as the limitation

recited in independent claims 25-28. None of the listed conditions, i.e., access privileges, request validity, and memory integrity validation, are irrevocable conditions.

Habersetzer fails to teach what Maillard lacks. Habersetzer discloses enabling and disabling access to IC test functions. According to Habersetzer, an IC is tested during fabrication using a test circuit. However, that test circuit is disabled when the IC is sold so that customers are prevented from entering the test mode. Since Habersetzer relates to a test circuit, Habersetzer fails to teach or suggest enabling or disabling access to a encryption key. Furthermore, Habersetzer fails to disclose that the circuit is irrevocably in one condition or the other. For example, the programmable logic devices at both the disable re-enable circuits allow the test mode circuit to undergo multiple iteratum (see col. 7, lines 35-39). Accordingly, dependent claims 25 and 28 are allowable over Millard in view of Habersetzer.

Cromer also fails to teach what Maillard lacks. Cromer relates to a computer system that is disabled when it is disconnected from a network (see, e.g. col. 2, line 66 to col. 3, line 2). The goal of Cromer is to prevent access to a computer hard drive if a computer is stolen and disconnected from its network. The Examiner states that Cromer makes the limitations of irrevocable conditions obvious. However, Cromer relates to access of data on a hard drive. Accordingly, neither Maillard, Habersetzer, nor Cromer disclose, teach or suggest enabling or disabling access to an encryption key stored on a recording device.

The Examiner does not specifically discuss Fielder and Reardon in his rejection of independent claims 25 and 28, except to list them. However, these references also fail to teach or suggest what Maillard lacks. Fielder relates to an encryption key generator system and method and fails to disclose a device for encrypting and recording a digital stream of data including a readout path for the unique key. Reardon describes a network security system in which a security gateway

generates a key pair for each user. However, Reardon does not specifically disclose a recorder having a unique key for recording a digital data stream or a readout path for reading a unique key of the device. In view of the above amendments and remarks, it is respectfully submitted that independent claims 25 and 28 are allowable over Maillard in view of Fielder, Reardon, Habersetzer, and Cromer.

Dependent claims 2-12, 14-24, 26-27, 29-30, and 32-34, each being dependent on one of independent claims 1, 13, 25, 28, and 31, are deemed allowable for the same reasons expressed above with respect to independent claims 1, 13, 25, 28, and 31.

Dependent claims 2 and 14 recite decrypting the encrypted packets in the recording and playback device according to the encryption key unique to the recording and playback device. Maillard fails to disclose decrypting the packets according to a decryption key unique to the apparatus. At col. 8, lines 47-52, of Maillard, the access control module 42 decrypts the EMM to determine the key $K_t$, which is used to decrypt the ECM to obtain the control word needed to unscramble the stored data. Accordingly Maillard does not decrypt the stored data. Rather, it decrypts the keys necessary to determine the control word used to scramble the data. Accordingly, claims 2 and 14 are allowable for these additional reasons.

Dependent claims 6 and 18 recite a packet comprises a first predetermined number of header bytes and a second predetermined number of payload bytes and the header bytes are stored unencrypted. Maillard discloses at col. 8, lines 30-35, that each recording requires a header 60. As shown in Fig. 4, Maillard discloses that only one heading is required for each recording, not for each packet (the right hand side of Fig. 4 in Maillard seems to show multiple packets after the header 60). Furthermore, the size of the header and segments are undefined in Maillard. Dependent claims 6 and 18 are allowable for these additional reasons.

Dependent claims 3-5, which correspond with claims 15-17 and 33-34, each recite that the encryption key includes a first portion hardwired in the recording and playback device, a second portion stored in a memory of the recording and playback device, and that the encryption key is formed in the recording and playback device. In contrast, Maillard discloses that the encryption of data is actually the encryption of a control word at a broadcast center. Maillard does not teach that the key has two parts. The only key unique to the recording device of Maillard is the $K_i$ which is used for encrypting the key $K_t$. Accordingly, Maillard fails to teach that one key has a plurality of parts. For all of these additional reasons, dependent claims 3-5, 15-17, and 33-34, are also allowable.

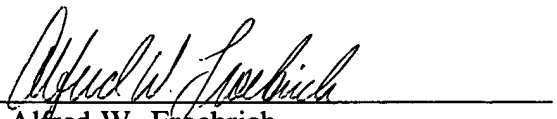
Dependent claims 8 and 20 recite that stored packets are retrieved, header bytes are replaced, and payload bytes are decrypted. As stated above, the headers of Maillard contain general information and not any status information of the packets. The recording of Maillard can not be considered a packet, as recited in the claims because it is a variable size. In contrasts, packets include a definite size. Accordingly, Maillard fails to disclose teach or suggest the limitations of claims 8 and 20.

The application is now deemed to be in condition for allowance and notice to that effect is solicited.

It is believed that no fees or charges are required at this time in connection with the present application. However, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By 

Alfred W. Froebrich
Reg. No. 38,887
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: November 8, 2004